OIPE JC17 NOV 12 2003 PATENT & TRADEMARK OFFICE

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Takanori MASUI et al.

Application No.: 10/653,219

Filed: September 3, 2003 Docket No.: 116972

For: APPARATUS AND METHOD FOR SECURELY REALIZING COOPERATIVE PROCESSING

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2003-082323 filed March 25, 2003

In support of this claim, a certified copy of said original foreign application:

☒ is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Thomas J. Pardini
Registration No. 30,411

JAO:TJP/tmw

Date: November 12, 2003

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年　３月２５日

出 願 番 号
Application Number: 特願２００３－０８２３２３

[ST. 10/C]: ［ＪＰ２００３－０８２３２３］

出 願 人
Applicant(s): 富士ゼロックス株式会社

２００３年１０月　３日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０８１８５１

【書類名】　特許願
【整理番号】　FE03-00391
【提出日】　平成15年 3月25日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/00
【発明者】
　【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社内
　【氏名】　益井　隆徳
【発明者】
　【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社内
　【氏名】　横濱　竜彦
【発明者】
　【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社内
　【氏名】　佐竹　雅紀
【特許出願人】
　【識別番号】　000005496
　【氏名又は名称】　富士ゼロックス株式会社
【代理人】
　【識別番号】　100075258
　【弁理士】
　【氏名又は名称】　吉田　研二
　【電話番号】　0422-21-2340

【選任した代理人】

【識別番号】　100096976

【弁理士】

【氏名又は名称】　石田　純

【電話番号】　0422-21-2340

【手数料の表示】

【予納台帳番号】　001753

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　情報処理装置及び方法

【特許請求の範囲】

【請求項１】　指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現する情報処理装置であって、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に電子署名を施す署名部と、

前記署名部により電子署名が施された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する送信部と、

を備えることを特徴とする情報処理装置。

【請求項２】　請求項１に記載の情報処理装置であって、

前記署名部は、サービスを依頼した依頼者の電子署名を施すことを特徴とする情報処理御装置。

【請求項３】　請求項１に記載の情報処理装置であって、

前記署名部は、自装置の電子署名を施すことを特徴とする情報処理装置。

【請求項４】　請求項３に記載の情報処理装置であって、

自装置は、サービスを発行する発行元装置であることを特徴とする情報処理装置。

【請求項５】　請求項３に記載の情報処理装置であって、

自装置は、一のジョブ処理装置と他のジョブ処理装置との間を中継してジョブ処理された結果を転送する中継装置であることを特徴とする情報処理装置。

【請求項６】　請求項１に記載の情報処理装置であって、

前記署名部は、　電子署名付与の対象とする処理記述より後に処理を実行すべき処理記述を含めて署名することを特徴とする情報処理装置。

【請求項７】　　請求項１記載の情報処理装置において、

前記署名部は、各ジョブ処理装置の実行対象となる複数の部分について、それぞれ電子署名を施すことを特徴とする情報処理装置。

【請求項８】　請求項１記載の情報処理装置において、

前記署名部は、処理記述の処理単位に電子署名を施すことを特徴とする情報処理装置。

【請求項９】　指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現するためにコンピュータが実行する情報処理方法であって、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に電子署名を施し、

電子署名が施された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する

ことを特徴とする情報処理方法。

【請求項１０】　指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現させるコンピュータのプログラムあって、

コンピュータに、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に電子署名を施す手順と、

電子署名が施された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する手順と

を実行させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワーク上に存在する様々な処理装置を連携させることで、多様な連携処理を実現するための技術に関し、特に連携処理におけるセキュリティ技術に関する。

【０００２】

【従来の技術】

スキャナ、ファクシミリ装置、プリンタ、複写機、及びそれらの機能を統合した複合機をＬＡＮ（ローカルエリアネットワーク）に接続し、パーソナルコンピ

ュータやメールサーバなどの情報処理装置と連携させ、オフィス作業用の各種サービスを提供するワークフローシステムが提案されている。

【０００３】

また近年、インターネット上に散在する各種ウェブアプリケーションを連携させる技術が提案されている。インターネット上にある多様な提供者が提供するアプリケーションサービスを連結して１つのシステムを構成できると、様々な既存サービスを利用することができるのでシステム開発コストが大幅に低減できると期待されている。また、このような連携的なサービスを実現するための共通の基盤としてＸＭＬ(eXtensible Markup Language)等の言語が注目されている。

【０００４】

また、従来のワークフローシステムとしては、特許文献１や特許文献２、特許文献３に示されるものが知られている。また、ワークフロートは無関係であるが、電子署名に関する従来技術として特許文献４に示すものがある。この文献には、プログラムコードをセキュアに実行するコンピュータシステムにおいて、暗号化したプログラムコードに対しメモリ割当の最小単位ごとに電子署名を付すことで、署名検証や復号の処理をマルチタスク実行可能とする点が示されている。

【０００５】

【特許文献１】

特開平０８－１２３７４４号公報

【特許文献２】

特開２００２－０９９６８６号公報

【特許文献３】

特開２００１－２８２９７０号公報

【特許文献４】

特開２００２－３５３９６０号公報

【０００６】

【発明が解決しようとする課題】

フローを構成する各処理装置に対するサービスの要求は、何らかの指示データをその処理装置に送ることにより行われる。ここで、指示データの改ざんや、な

りすましなどの危険性があると、処理装置側が要求するセキュリティレベルを満足できない場合が出てくる。

【０００７】

現在のインターネット技術では、データの改ざん等の危険性を軽減する手段として、ＰＫＩ（公開鍵基盤）における電子署名が用いられている。ところが、ワークフロー等の連携サービスでは、単なる電子署名技術だけでは以下のような理由から十分でない場合がある。

【０００８】

すなわち、処理装置にとっては、受け取った指示データが、連携サービスの要求者による指示内容の通りか否かが１つの重要な問題になる。ここで、ある処理装置が自分の受け取った指示データに対して加工を加えて次の処理装置に伝達するようなフローの仕組みも考えられるが、この仕組みでは、サービス要求者が最初に指示データに付した電子署名がフローの途中の処理装置で失われてしまうという問題がある。

【０００９】

【課題を解決するための手段】

本発明は、指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現する情報処理装置であって、前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に電子署名を施す署名部と、前記署名部により電子署名が施された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する送信部とを備える情報処理装置を提供する。

【００１０】

また本発明の好適な態様では、前記署名部は、サービスを依頼した依頼者の電子署名を施す。また別の好適な態様では、前記署名部は、当該情報処理装置の電子署名を施す。

【００１１】

また本発明のある態様では、前記情報処理装置は、前記サービスを発行する発行元装置である。例えば、発明の実施の形態の指示入力装置がこの発行元装置の

一例である。

【００１２】

また別の態様では、前記情報処理装置は、一のジョブ処理装置と他のジョブ処理装置との間を中継してジョブ処理された結果を転送する中継装置である。例えば発明の実施の形態におけるフロー制御装置が、この中継装置の一例である。

【００１３】

また本発明の好適な態様では、前記署名部は、電子署名付与の対象とする処理記述より後に処理を実行すべき処理記述を含めて署名する。

【００１４】

【発明の実施の形態】

以下、本発明の実施の形態（以下実施形態という）について、図面に基づいて説明する。

【００１５】

図１は、本発明に係るサービス提供システムのシステム構成パターンの一例を示す図である。このシステムは、指示入力装置１０、フロー制御装置２０、及び複数のアプリケーションサーバ２５を含んでいる。

【００１６】

アプリケーションサーバ２５は、他の装置からの要求に応じて所定の処理サービスを提供するサーバである。例えば、サーバ２５の例としては、例えば、文書データベースサーバや、メールサーバ、画像データに対して色変換や回転などの操作を施す画像処理サーバ等を挙げることができる。サーバ２５は、そのような処理サービスを例えばウェブアプリケーションサービス等の形で提供する。

【００１７】

このシステムは、あるサーバ２５で文書を検索し、この結果検索された文書を別のサーバによって電子メールとして送信する、といった具合に、複数のサーバ２５の処理を連携させた連携サービスを提供することができる。

【００１８】

指示入力装置１０は、このシステムに対するユーザの処理指示を入力するための装置である。ユーザは、指示入力装置１０に対し、上述のような連携サービス

の実行指示を入力することができる。指示入力装置１０は、例えばパーソナルコンピュータに、ユーザから本システムへの指示の入力を受け付けるためのユーザインタフェースプログラムを組み込んだものでよい。しかしながら、オフィスにおける文書処理サービスを想定すると、情報処理機能や通信機能に加え、紙文書を読み取って電子データ化する機能をも備えるデジタル複合機を指示入力装置１０として用いることが好適である。デジタル複合機は、スキャナ、プリンタ、複写機、ファクシミリ、ネットワーク通信等の機能を併せ持つ。

【００１９】

フロー制御装置２０は、各サーバ２５に対して処理を依頼することで、それら個々のサーバ２５が提供するサービスを連携した連携サービスを実現する。

【００２０】

好適には、指示入力装置１０、フロー制御装置２０及び各サーバ２５は、公開鍵暗号方式に対応しており、各自の秘密鍵、公開鍵を有している。また、指示入力装置１０、フロー制御装置２０及び各サーバ２５は、他の装置１０，２０やサーバ２５の公開鍵を保持しているか、又は必要に応じてネットワーク上の認証局から取得することができる。

【００２１】

図１のシステムでは、ユーザが指示入力装置１０に対して連携サービスの指示を入力すると、指示入力装置１０がその指示内容を示したデータを送る。このデータを、以下ではフロー指示書５０と呼ぶ。このフロー指示書５０には、連携サービスに関与するすべてのサーバの処理内容の記述と、それら各処理の実行順序の情報が含まれている。フロー指示書５０を受信したフロー制御装置２０は、その指示書５０に従って各サーバ２５を制御することで、その指示書５０が示す連携サービスを実現する。

【００２２】

このとき、フロー制御装置２０は、受信したフロー指示書５０に基づき各サーバ２５への指示書（指示内容を示したデータ）５２を作成し、これら指示書５２を各サーバ２５に送ることで、それらサーバ２５の連携動作を実現する。すなわち、フロー制御装置２０は、フロー指示書５０の記述に従い、次に動作させるべ

きサーバ２５に対して指示書５２を送信し、これに対してそのサーバ２５から処理終了の通知（及び場合によっては処理結果のデータ）が返ってくると、その次のサーバ２５に対して指示書５２を送信する。

【００２３】

このように図１のシステムは、サーバ２５群がフロー制御装置２０の制御の下に連携するという、いわばスター（星）型のシステム構成をとっている。

【００２４】

次に、図２を参照して、本発明に係るサービス提供システムのシステム構成パターンの別の一例を説明する。図２において、図１に示したシステムの構成要素と同等の構成要素には同一符号を付して説明を簡略化する。

【００２５】

このシステムは、指示入力装置１０と複数のアプリケーションサーバ２５とから構成されている。

【００２６】

図１のシステムが連携制御のためのフロー制御装置２０を有するのに対し、図２のシステムはそのような中央の制御装置を持たず、各アプリケーションサーバ２５自身が連携動作のための制御動作を実行する。このため、指示入力装置１０は、ユーザが指示した連携サービスのために各サーバ２５が実行すべき処理を示したフロー指示書５０を作成し、これを各サーバ２５に送信して実行させる。

【００２７】

図２の構成は、連携サービスを構成する各処理のための各サーバ２５が、それら各処理の順に並んだ、いわばデイジーチェーン（連鎖）型の構成となる。この構成では、サーバ連鎖の中の最初のサーバ２５－１に対して指示入力装置１０から指示書５０を送信すると、これを契機にサービス処理が開始される。そして、サーバ２５－１の処理が終了すると次のサーバ２５－２の処理が開始され、このサーバ２５－２の処理が終了するとその次のサーバ２５－３の処理が開始されるといった具合に、各段階のサーバ２５の間で処理が連携されていく。この場合、各サーバ２５には、指示入力装置１０から直接、又は前段のサーバ２５から指示書５４が送信される。そして、各サーバ２５はその指示書に従って処理を実行す

るとともに、その指示書に示された次のサーバ２５に対して処理開始の指示又は指示書５４を送信する。このような仕組みで連携が実現される（詳細は後述）。

【００２８】

以上、各サーバ２５の連携の仕組みとして、フロー制御装置２０により集中制御するフロー制御装置介在型と、各サーバ２５が順に次のサーバ２５に処理を受け渡すデイジーチェーン型の２つの仕組みを説明した。

【００２９】

次に、連携サービスのために各サーバ２５に送信される指示書５２，５４についての２つのタイプを説明する。

【００３０】

第１は、連携サービスに関与する各サーバ２５に対し、当該サーバ２５への指示（該サーバ２５の処理内容の記述）のみならず、他のサーバ２５への指示をも含んだ指示書５２又は５４を送信する方式である。この方式の１つの例として、連携サービスに関与するすべてのサーバ２５への指示を含んだ指示書を各サーバ２５に送信する方式がある。このように、他のサーバ２５への指示も含む形態の指示書を「包括指示書」と呼ぶこととする。

【００３１】

第２は、連携サービスに関与する各サーバ２５に対し、当該サーバ２５への指示のみを含み、他のサーバ２５への指示を含まない指示書５２又は５４を送信する方式である。このように、当該サーバ２５への指示のみからなる指示書を「個別指示書」と呼ぶこととする。

【００３２】

これら指示書５２又は５４の２つのタイプと、前述のシステム構成の２つのタイプを組み合わせれば、各サーバ２５への指示書の送信形態としていくつかの送信形態が得られる。そのうちの代表的なものとして次の２つの指示送信形態を挙げることができる。

【００３３】

まず第１は、図３に示すようなフロー制御装置介在型システムにおける指示送信形態である。

【００３４】

この指示送信形態では、まず指示入力装置１０からフロー制御装置２０に対し、サービスのために利用するすべてのサーバ２５－１，２５－２，２５－３に対する個別指示書６２－１，６２－２，６２－３を含んだ包括指示書６０が送信される。１つの例では、包括指示書６０には、それら個別指示書６２－１，６２－２，６２－３が、実行される順序に配列されている。フロー制御装置２０は、受信した包括指示書６０から各個別指示書６２－１，６２－２，６２－３を取り出し、これらを対応するサーバ２５－１，２５－２，２５－３にそれぞれ必要なタイミングで送信する。

【００３５】

第２の指示送信形態は、フロー制御装置非介在型システムに包括指示書を適用したものである。この形態の一例を図４に示す。

【００３６】

図４の形態では、まず指示入力装置１０からフロー中の最初のサーバ２５－１に対し、サービスのために利用するすべてのサーバ２５－１，２５－２，２５－３に対する個別指示書６２－１，６２－２，６２－３を含んだ包括指示書６０が送信される。これを受け取ったサーバ２５－１は、包括指示書６０から自分宛の個別指示書６２－１を識別し、これに従って処理を実行する。そしてサーバ２５－１は、その包括指示書６０から自分宛の個別指示書６２－１を削除して新たな包括指示書６０ａを作成し、これをフロー中の次のサーバ２５－２に送信する。次のサーバがどれかは包括指示書６０内に記述されている。包括指示書６０ａを受信したサーバ２５－２も同様に動作し、その包括指示書６０ａから自分宛の個別指示書６２－２を削除して包括指示書６０ｂを作成し、次のサーバ２５－３に送る。このように第２の指示送信形態では、各サーバ２５が包括指示書６０から自分宛の個別指示書６２を順次削除して次のサーバ２５に受け渡していく。

【００３７】

上記第１及び第２の指示送信形態ではいずれも、指示入力装置１０に対しユーザが連携サービスの実行を指示したとき、作成した包括指示書６０のデータに対してそのユーザやその指示入力装置１０の秘密鍵を用いて電子署名を施すことが

可能である。このため、その包括指示書６０を直接受け取るフロー制御装置２０やサーバ２５－１なら署名検証によりその指示書６０の改ざんの有無等を確認できる。このように、サービスを要求するユーザ自身の秘密鍵を用いて作成した電子署名や、その要求の入力に用いた指示入力装置１０の秘密鍵を用いて作成した電子署名をイニシエータ(initiator)署名と呼ぶことにし、そのユーザ及び指示入力装置１０をイニシエータと総称することとする。イニシエータ署名として、ユーザの電子署名と指示入力装置１０の電子署名のいずれを要求するかは、連携サービスのシステムや、そのシステムに参加する各サーバ２５のセキュリティーポリシーによる。セキュリティーポリシーによっては、イニシエータ署名としてそれら両方の電子署名を施すことも考えられる。

【００３８】

これに対し、包括指示書６０のデータから各サーバ２５宛の個別指示書６２や包括指示書６０ａ、６０ｂを作成した場合、それら新たに作成した指示書にとっては、元の指示書６０に付されていたイニシエータ署名は無効となってしまう。このため、フロー制御装置２０や別のサーバ２５を介して指示書を受け取るサーバ２５は、その指示書がイニシエータからの正しいものなのかを検証することができない。

【００３９】

以上のようなイニシエータ署名についての問題を解決するための本実施形態の仕組みを、以下に説明する。

【００４０】

この仕組みの基本的な考え方は、指示入力装置１０が包括指示書６０を作成する際、その包括指示書６０に組み込む各サーバ２５宛の個別指示書６２に対し、それぞれ個別にイニシエータ署名を施すというものである。

【００４１】

この考え方に従った、図３の指示送信形態に好適な包括指示書の構成を、図５を参照して説明する。

【００４２】

図５に示す包括指示書７０は、図３，４に示した包括指示書６０に対応するも

のであり、３つのサーバ２５－１，２５－２，２５－３への各署名済み個別指示書７２－１，７２－２，７２－３を含んでいる。各署名済み個別指示書７２－１，７２－２，７２－３は、平文の個別指示書６２－１，６２－２，６２－３に対してそれぞれイニシエータ署名７４－１，７４－２，７４－３を付加したものである。

【００４３】

このような包括指示書７０を用いた場合、フロー制御装置２０は、包括指示書７０から各署名済み個別指示書７２－１，７２－２，７２－３を取り出して対応するサーバ２５－１，２５－２，２５－３に送信することになる。各サーバ２５は、受信した署名済み個別指示書７２に含まれるイニシエータ署名７４を検証することで、その個別指示書７２の真正性等を検査できる。

【００４４】

また、図５の包括指示書７０には、これら署名済み個別指示書７２－１，７２－２，７２－３の全体に対するイニシエータ署名７６が含まれている。この全体に対するイニシエータ署名７６は、指示入力装置１０からこの包括指示書７０を受信したフロー制御装置２０が、その指示書７０の真正性等を検証するのに用いられる。また、この全体に対するイニシエータ署名７６は、個々の署名済み個別指示書７２－１，７２－２，７２－３の流用を防ぐためにも効果がある。

【００４５】

すなわち、本実施形態の方式では、包括指示書７０に含まれている個別指示書７２にイニシエータ署名７４が付されているので、例えばインターネット上の第三者が、様々な包括指示書７０を集めてそれらから署名済み個別指示書７２を取り出し、再組み立てして別の包括指示書を作成し不正利用するおそれがある。これに対し、図５の例にように、包括指示書７０中に含まれるすべての署名済み個別指示書７２を併せたものに対してイニシエータ署名７６を付加すれば、そのような不正な再組み立てによって作成された包括指示書は、フロー制御装置２０での署名検証で検出できるので、不正利用を防止できる。

【００４６】

なお、包括指示書７０から取り出した署名済み個別指示書７２をサーバ２５に

直接送るという方法での不正利用も考えられる。しかしながら、これに対しては、フロー制御装置２０が署名済み個別指示書７２に対して当該装置２０自身の秘密鍵で電子署名を付加し、サーバ２５側でその装置２０の電子署名を検証することで、そのような不正を検出できる。

【００４７】

次に、この包括指示書７０の具体例を説明する。

【００４８】

ここでは、説明のために、指示入力装置１０で読み取った複数のページを有する文書ファイルから第１ページのデータを取り出し、所定の宛先に電子メールで送信するという連携サービスを表す包括指示書を考える。包括指示書が使用されるシステムとしては、図３に示したフロー制御装置介在型のシステムを考える。このシステムにおいて、サーバ２５－１がページばらし（文書ファイルをページ単位のファイルに分割し、要求されたページのファイルを返す処理）のサービスを提供し、サーバ２５－２が電子メール送信サービスを提供するものとする。またサーバ２５－１は"pagedivider.foo.jp"というホスト名を有し、サーバ２５－２は"mailsender.foo.jp"というホスト名を有するとする。この指示書７０に示される連携サービスでは、指示入力装置１０にて紙原稿の読み取りが行われ、サーバ２５－１にて読み取り結果の文書ファイルから第１ページが抽出され、サーバ２５－２にてその第１ページのファイルを含んだ電子メールが作成され、所定宛先に送られることになる。

【００４９】

このような連携サービスを記述した平文の包括指示書６０は、図６に示すような記述となる。

【００５０】

図６の包括指示書６０は、ＸＭＬ(eXtended Markup Language)で記述されている。この包括指示書６０は、この指示書６０で使用しているＸＭＬのバージョンや文字コードを示す文書要素６０５と、この指示書６０が表す連携サービスを示す文書要素６１０とを含んでいる。連携サービスを示す要素６１０のタグには、この連携サービスの名称（name="report delivery"）が示されている。そして、

この要素６１０には、それら連携サービスを担う各サーバ２５－１，２５－２に対する個別指示書６２０ａ，６２０ｂとが記述されている。

【００５１】

個別指示書６２０ａの記述６２２ａには、連携サービス中での当該処理の順番（order="1"）、及び当該処理を実行するサーバ２５－１のホスト名（url="pagedivider.foo.jp"）が示されている。また、記述６２４ａの１行目には、そのサーバ２５－１が提供する各種の処理のうち、今回利用する処理の名称（jobname="ExtractFrontPage"）が示される。例えば、サーバ２５－１は、文書ファイルから先頭ページを取り出してその先頭ページのファイルを作成する処理の他に、文書ファイルをページ単位にばらして各ページごとのファイルを作成する処理などの様々な処理ができる。記述６２４ａの１行目は、それら様々な処理のうち、文書ファイルの先頭ページのファイルを作成する処理を示すものである。また記述６２４ａの２行目及び３行目にはその処理のパラメータが示されている。２行目のパラメータは、その処理に対する入力ファイルのファイル名（"ExtractFrontPage"）を示し、３行目のパラメータはその処理の出力ファイルのファイル名（"ExtractedPage"）である。指示入力装置１０が、読み取った原稿を示す文書ファイルに対し、"ExtractFrontPage"と言うファイル名を付し、この指示書６０に添付して送信すれば、サーバ２５－１でそのファイルが処理対象であると認識できる。

【００５２】

また、個別指示書６２０ａは、この指示書が示す処理の後に処理を行うサーバ２５－２を示す記述６２６ａを含んでいる。この記述６２６ａには、次のサーバ２５－２のホスト名（url="pagedivider.foo.jp"）が示されている。

【００５３】

サーバ２５－２に対する個別指示書６２０ｂは、上記個別指示書６２０ａと同様、処理の順序及びサーバ２５－２のホスト名を示す記述６２２ｂと、そのサーバ２５－２が行うべき処理の名称及びその処理のパラメータを示す記述６２４ｂを含んでいる。サーバ２５－２が行う処理は、電子メールの送信処理なので、パラメータとしては電子メールの宛先アドレス（記述６２４ｂの２行目）と、その

電子メールに添付されるファイルの名称（記述６２４ｂの３行目）とを含んでいる。なお、添付されるファイルの名称は、サーバ２５－１の処理の出力ファイル名と同じものとなっている。

【００５４】

なお、サーバ２５－２は、この包括指示書６０が示す連携サービスの中の最後の処理なので、次のサーバを示す記述は含まれていない。

【００５５】

このような平文の包括指示書６０に対するに、図５に示した考え方に従ってイニシエータ署名を施した包括指示書７０の記述は図７に示すようなものとなる。なお、図７の例は、説明のために簡略化を行っている。

【００５６】

図７の記述例では、包括指示書７０は、サーバ２５－１に対する署名済み個別指示書７２０と、サーバ２５－２に対する署名済み個別指示書７３０を含んでいる。

【００５７】

サーバ２５－１宛の署名済み個別指示書７２０は、<Signature> タグ７２２で示されるエンベローピング署名形式の署名要素として記述される。この署名要素の中には、まず電子署名に用いたアルゴリズムなどの情報を示す署名情報要素７２６が記述される。この例では署名アルゴリズムとしてＳＨＡ－１(RFC3174)が用いられている。その次に<object>，</object>タグで挟まれた署名対象要素Ｓが記述される。この署名対象要素Ｓは、平文の包括指示書６０の個別指示書６２０ａ（図６参照）と同じ記述内容である。また、要素７２４は、署名対象要素Ｓに対し、イニシエータの秘密鍵と指定された署名アルゴリズムから求めた署名値を示す署名値要素である。図７では省略しているが、署名済み個別指示書７２０内には、署名値要素７２４を計算するのに用いた秘密鍵に対応する公開鍵を示す鍵情報要素（<KeyInfo>タグで示される）が含まれる。後段のサーバがその署名を検証する場合は、その鍵情報要素の情報に基づき、署名鍵に対応する公開鍵を取得し、この公開鍵を用いて署名検証を行うことになる。

【００５８】

同様に、サーバ２５－２宛の署名済み個別指示書７３０は、タグ７３２で示される署名要素内に、署名情報要素７３６、署名対象要素Ｔ（個別指示書６２０ｂ）、その要素Ｔに対するイニシエータ署名値を示す署名値要素７３４及び鍵情報要素が含まれる。

【００５９】

そして、包括指示書７０全体は、これら２つの署名済み個別指示書７２０及び７３０をマージした署名対象要素Ｕに対し、イニシエータ署名を施したものとなる。すなわち、包括指示書７０は、<Signature> タグ７１２で示される署名要素の中に、署名情報要素７１６、署名対象要素Ｕ、及びその要素Ｕに対するイニシエータ署名値を示す署名値要素７１４及び鍵情報要素を含んだものとなる。

【００６０】

次に、図４に示した第２の指示送信形態に好適な包括指示書の構成を、図８を参照して説明する。

【００６１】

図８の包括指示書８０では、まず各個別指示書６２－１，６２－２，６２－３が、それぞれイニシエータ署名８４－１，８４－２，８４－１を付されることで、署名付き個別指示書８２－１，８２－２，８２－３となっている。更に、連携サービス中での処理順序が最後の署名付き個別指示書８２－３と１つ前の署名付き個別指示書８２－２とをマージ（併合）した記述に対してイニシエータ署名８７を付すことで、ブロック８５が形成されている。そして、このブロック８５にもう１つ前（そしてこの例では指示書中の先頭）の署名付き個別指示書８２－１をマージした記述に対し、イニシエータ署名８８が付されている。この最外郭のイニシエータ署名８８は、図５の構成における包括指示書全体に対するイニシエータ署名７６に対応する。

【００６２】

このようにイニシエータ署名が入れ子的に施された包括指示書８０は、各署名付き個別指示書８２－１，８２－２，８２－３に対し、処理順序の逆順に、「署名結果に対し１つ前の署名付き指示書をマージしてイニシエータ署名を施す」という処理を再帰的に適用することで作成することができる。すなわち、この署名

処理では、電子署名付与の対象とする処理記述（すなわち個別指示書）より後に処理を実行すべき処理記述を含めて署名している。

【００６３】

指示入力装置１０でこのような包括指示書８０を作成し、最初のサーバ２５－１に送信すると、そのサーバ２５－１は、まず包括指示書８０全体に対するイニシエータ署名８８を検証する。この検証が成功した場合、サーバ２５－１は、自分宛の署名付き個別指示書８２－１を探し、その指示書８２－１のイニシエータ署名８４－１を検証する。この検証が成功すると、サーバ２５－１は、その指示書８２－１の記述に従って処理を実行すると共に、次のサーバ２５－２宛の包括指示書８０ａを作成する。この包括指示書８０ａは、基となる包括指示書８０から、サーバ２５－１宛の署名付き個別指示書８２－１と最外郭のイニシエータ署名８８を取り除いて残るブロック８５に対し、ＸＭＬフォーマットの包括指示書として必要なタグ等を付加することにより作成される。すなわち、包括指示書８０ａでは、ブロック８５のイニシエータ署名８７が、包括指示書８０ａ全体に対するイニシエータ署名となる。

【００６４】

次に、包括指示書８０ａを受け取ったサーバ２５－２も、同様に指示書８０ａ全体のイニシエータ署名、及び自分宛の署名付き個別指示書８２－２のイニシエータ署名を検証し、それら検証が共に成功すれば、その指示書８２－２の処理を実行し、その次のサーバ２５－３宛の包括指示書８０ｂを作成する。この包括指示書８０ｂも、上記と同様、基となる包括指示書８０ａから署名付き個別指示書８２－２と最外郭のイニシエータ署名８７を取り除き、この結果残る署名付き個別指示書８２－３に対し、包括指示書として必要なタグ等を付加することにより作成される。

【００６５】

サーバ２５－３は、その包括指示書８０ｂを受け取ると、その中に含まれる自分宛の署名付き個別指示書８２－３のイニシエータ署名を検証し、検証が成功すると、その指示書に示される処理を実行する。これにより、包括指示書８０に対応する連携サービスが完了する。

【００６６】

このように、図８に示す入れ子構造の包括指示書８０では、連携サービスのフロー中のどのサーバ間をとっても、前のサーバ２５から次のサーバ２５に受け渡す指示書の基になるデータブロック（すなわち該次のサーバ以降の各サーバへの指示書群）全体に対し、イニシエータ署名が必ず付されていることになる。したがって、各サーバ２５は、前のサーバ２５から受け取った包括指示書から、自分宛の個別指示書を取り除くことで、次のサーバ２５に対し、全体に対するイニシエータ署名が付いた包括指示書を作成できる。

【００６７】

したがって、図８の包括指示書８０の構造でも、サーバ２５から次のサーバ２５に送られる包括指示書は、常にその包括指示書全体に対してイニシエータ署名が付されているので、第三者が個々の署名付き個別指示書８２を再組み立てして包括指示書を作成するといった不正行為を防止することができる。

【００６８】

次の、図８の包括指示書８０の具体例を、図９を参照して説明する。

【００６９】

図９の具体例は、指示入力装置１０で読み取った複数のページを有する文書ファイルから第１ページのデータを取り出し（サービスＡ）、それを所定のファイルフォーマットに変換（サービスＢ）してから、所定の宛先に電子メールで送信する（サービスＣ）という、３つのサービスからなる連携サービスを表す。これら３つのサービスのうち、サービスＡ及びＣは、図６及びの例におけるページばらし及び電子メール送信と同じ処理内容なので一部の記述を省略している。

【００７０】

図９の記述例では、各署名付き個別指示書８２０，８３０，及び８４０に対し、それぞれ署名対象要素Ｖ，Ｗ，Ｘに対するイニシエータ署名８２４，８３４，及び８４４が付されている。そして、署名付き子個別指示書８３０と８４０とを併合した署名対象要素Ｙに対し、イニシエータ署名８５４が付されている。そして、署名対象要素Ｙとイニシエータ署名８５４からなる署名要素８５０にその前の署名付き個別指示書８２０を併合した署名対象要素Ｚに対し、イニシエータ署

名８１４が付されることで、全体としての包括指示書８０が構成されている。

【００７１】

以上、図３及び図４の各指示送信形態に対応する包括指示書７０及び８０のデータ構造を説明した。図７及び図９に示した包括指示書７０及び８０の記述は、ＸＭＬ-signature（RFC3275）のエンベロービング(enveloping)署名形式を用いた場合の例である。しかしながら、当業者ならば明らかなように、本実施形態の方式は、署名形式に依存するものではない。また更には、本実施形態の方式は、ＸＭＬなどといった指示書のデータフォーマットに依存するものでもない。

【００７２】

以上、本実施形態の署名処理について説明した。本実施形態は、指示書に対する電子署名に関するものであるため、暗号化などの側面については触れずに説明してきた。しかしながら、当業者ならば明らかなように、上述の本実施形態の署名処理を、必要に応じて暗号化処理と組み合わせることは可能である。例えば、各個別指示書６２０ａや６２０ｂの処理内容の記述６２４ａや６２４ｂ（図６参照）に対し、それぞれその個別指示書の宛先であるサーバの公開鍵で暗号化処理を施し、その暗号化結果に対してイニシエータ署名を施すことで、署名付き個別指示書を作成することもできる。また、逆に署名付き個別指示書に対して宛先サーバの公開鍵で暗号化を施すこともできる。

【００７３】

以上、本実施形態のシステムの構成及び動作について説明した。以上の実施形態では、第１段階として、連携サービスのために連携動作する各サーバへの個別指示書に対し、それぞれ個別にイニシエータ署名を施した。このときの署名処理の単位となる「サーバ」は、あるサービス処理を記述したアプリケーションプログラムをコンピュータで実行させることにより実現される仮想機械であってもよいし、そのようなアプリケーションプログラムを１乃至複数備えたハードウエア装置であってもよい。前者の場合は、アプリケーションごとの処理の記述が１つの個別指示書となるのに対し、後者の場合は１つのハードウエア装置に含まれる複数のアプリケーションの処理の記述を順に並べたものが１つの個別指示書となる。

【００７４】

次にこのシステムを構成する指示入力装置１０，フロー制御装置２０及び各サーバ２５の内部構成の一例を、図１０を参照して説明する。

【００７５】

まず、指示入力装置１０について説明する。指示入力装置１０のＵＩ（ユーザ・インタフェース）１０２は、指示入力装置１０の状態や操作メニュー等を表示し、これに対するユーザの選択やパラメータ入力を受け取るユーザ・インタフェース機構であり、例えば液晶タッチパネルやテンキーボタン、各種の指示ボタンを備える。処理モジュール１０４は、当該指示入力装置１０自体がユーザに提供するサービス処理を実行する処理モジュールである。指示入力装置１０が複合機である場合、処理モジュール１０４には、スキャン機能、プリント機能、コピー機能、ファクシミリ送受信機能等を実現する機能モジュールが含まれる。この場合、これら処理モジュール１０４は、スキャンエンジンやプリントエンジン、ファクシミリ装置等のハードウエアと、それら各ハードウエアを制御するソフトウエアの組合せにより構成される。通信制御部１０６は、この指示入力装置１０とＬＡＮ等のネットワーク３５上の他の装置との通信のための各種制御処理を行う機能モジュールである。

【００７６】

暗号・復号処理部１０８は、指示入力装置１０からネットワーク３５に送信するデータに対して暗号化を行ったり、送信されてきた暗号化されたデータを復号したりする機能モジュールである。ここでは、暗号・復号処理部１０８は、暗号方式として公開鍵暗号方式をサポートしているものとする。ただし、これは一例であり、暗号・復号処理部１０８は、共通鍵方式など他の暗号方式を基礎とするものであってもよい。

【００７７】

暗号・復号処理部１０８で用いる暗号化処理の一例としては、乱数等で発生したセッション鍵（共通鍵）を用いて対象となる文書データを暗号化し、このセッション鍵を送信先の公開鍵で暗号化し、これら両暗号化データを送信先へに送信するという処理を挙げることができる。受信側では、受け取ったデータを自らの

秘密鍵で復号することでセッション鍵を得、暗号化された文書データをそのセッション鍵により復号する。本明細書中で「公開鍵で暗号化する」といった場合、文字通り公開鍵を用いて対象データを暗号化する場合のみならず、このようなセッション鍵を利用する暗号化処理の場合もあるものとする。

【００７８】

また、暗号・復号処理部１０８は、送信するデータに対して電子署名を施したり、受信したデータに付された電子署名を検証したりする機能を備える。電子署名は、例えば署名対象の文書データからＳＨＡ－１やＭＤ５(RFC1321)等の所定ダイジェスト方式に従って求めたメッセージダイジェストを、署名者の秘密鍵で暗号化することにより得られる。この電子署名の検証は、該署名データを署名者の公開鍵で復号し、その復号化結果が、署名対象の文書データから所定ダイジェスト方式に従って求めたメッセージダイジェストと一致するか否かを判定することにより行われる。一致すれば、該文書データが署名者からの真正なデータであることが証明されると共に、該文書データに対して改竄が加えられていないことが証明される。

【００７９】

上述した本実施形態の電子署名処理は、この暗号・復号処理部１０８にて実行される。

【００８０】

ここで暗号・復号処理部１０８は、少なくともフロー制御装置２０の公開鍵を保管している。また暗号・復号処理部１０８に、各サーバやユーザの公開鍵をネットワーク上の所定の認証局等から必要に応じて取得する機能を設けることも好適である。また暗号・復号処理部１０８は、該指示入力装置１０自身の秘密鍵を備え、該指示入力装置１０の電子署名を行うことができる。

【００８１】

トークンＩ／Ｆ（インタフェース）１１０は、ユーザが保持するハードウエアトークンを受け入れ、このトークンと通信することで該ユーザの秘密鍵による電子署名を取得する機構である。ここでハードウエアトークンは、ユーザが携帯する小型の認証デバイスである。公開鍵暗号方式を利用する場合、ハードウエアト

ークンは、例えば、ユーザの秘密鍵データを記憶する記憶チップと、署名対象のデータに対してユーザの秘密鍵を用いて暗号化を施すことにより署名データを生成する演算回路と、署名対象のデータの入力及び署名データの出力のためのインタフェース機構とを備えるものとなる。ハードウエアトークンは、例えば接触読み取り式又は非接触読み取り式のＩＣカード、ＵＳＢ(Universal Serial Bus)等の各種有線インタフェース規格に対応したデバイス、或いはBluetooth等の各種無線インタフェース規格に対応したデバイスなどとして構成される。

【００８２】

包括指示書に対するイニシエータ署名として、サービスを依頼するユーザの電子署名が要求される場合は、このトークンＩ／Ｆ１１０を介してユーザのハードウエアトークンからイニシエータ署名の付与を受ける。

【００８３】

この構成では、通信制御部１０６は、送信すべきデータに対してユーザの電子署名を行う必要がある場合、例えばＭＤ５などの方式に従ってそのデータのメッセージダイジェストを作成し、これをトークンＩ／Ｆ１１０に装着されたハードウエアトークンに入力する。ハードウエアトークンは、入力されたメッセージダイジェストを、保持しているユーザの秘密鍵で暗号化し、その暗号化処理結果（すなわちユーザの署名）を通信制御部１０６に返す。このユーザ署名を通信制御部１０６が文書データに付加することにより、文書データに対するユーザの電子署名が為される。

【００８４】

以上ではユーザのハードウエアトークンを利用してユーザの電子署名を行う方式を説明したが、別の方式として、指示入力装置１０内にユーザの秘密鍵を予め保管しておき、この秘密鍵を用いて上述と同様の処理により該ユーザの電子署名を行う方式も可能である。この方式では、ユーザの秘密鍵保護のため、ユーザにパスワードやバイオメトリクス等の認証情報の入力を求め、これによりユーザ認証が成功した場合に限り、そのユーザの電子署名を認めるという制御を必須とする。ハードウエアトークンを用いる構成の場合、ユーザ署名が必要な連携サービスを行うと、最悪の場合その連携サービスが完了するまで指示入力装置１０にト

ークンをセットしたまま待っている必要があるが、指示入力装置１０に秘密鍵を保管する構成ではそのような待機は必要ない。逆に、ハードウエアトークンを用いる構成は、ユーザは、どの複合機その他の装置からでも、ユーザ署名が必要な連携サービスを実行できるという利点がある。

【００８５】

以上、指示入力装置１０の構成の一例を説明した。このような指示入力装置１０は、コンピュータや上述の複合機など、プログラムを実行して情報処理を実行することができる装置に、上述の各種の機能を記述したプログラムを実行させることによって実現できる。

【００８６】

次に、フロー制御装置２０の構成について説明する。これは、上述の第１の指示送信形態（図３）に対応するものであり、第２の指示送信形態（図４）の場合は、このフロー制御装置２０は必要ない。

【００８７】

フロー制御装置２０において、ユーザ管理部２０２は、該サーバ２０がサービス対象とするユーザについての各種情報を管理している。ユーザ管理部２０２が管理する情報には、例えばユーザの認証に用いる認証情報（パスワードやバイオメトリクス情報など）や、ユーザが登録しているＵＩ画面情報などがある。すなわち、本実施形態のシステムでは、ネットワーク３５上の各種サーバ装置が提供するサービスをユーザが組み合わせることで、ユーザ固有の連携サービスを定義可能としており、これらユーザ固有の連携サービスを指示できる該ユーザ固有のＵＩ画面をフロー制御装置２０から提供する。

【００８８】

この場合、ユーザ（個人の場合もあれば、複数人からなるグループの場合もある）が指示入力装置１０に認証情報を入力して認証が成功すると、指示入力装置１０がフロー制御装置２０に当該ユーザのＵＩ画面を要求する。この要求に応じ、フロー制御装置２０は、そのユーザが登録した連携サービスのメニュー等を含んだＵＩ画面を、そのユーザの公開鍵で暗号化した上で指示入力装置１０に送信する。ユーザが、指示入力装置１０のディスプレイに表示されたそのＵＩ画面上

で、使用したい連携サービスを選択すると、その選択内容がフロー制御装置２０の公開鍵で暗号化された上で、指示入力装置１０からフロー制御装置２０に送られる。この選択結果を受けとったフロー制御装置２０は、ユーザが選択した連携サービスを示す包括指示書のひな形データを、ユーザの公開鍵で暗号化した上で、指示入力装置１０に送信する。指示入力装置１０は、この包括指示書のひな形の中に、ユーザが入力しなければならないパラメータが含まれる場合、そのパラメータの入力画面をＵＩ１０２に表示し、ユーザの入力を求める。このようにしてパラメータ群が入力されると、包括指示書が完成する。これが上述のフロー指示書５０に対応する。指示入力装置１０は、完成したフロー指示書をフロー制御装置２０の公開鍵で暗号化した上で、フロー制御装置２０に送信する。

【００８９】

ユーザによるフロー制御装置２０への連携サービスの登録処理や、フロー制御装置２０から指示入力装置１０に提供する各ユーザ固有のＵＩ画面の情報については、本実施形態の要旨とは直接関係しないので説明を省略するが、これらについては本出願人による特願２００２－２７５２２９号、特願２００２－２７５２３０号、特願２００２－２７５２３１号に開示されているので、必要があれば参照されたい。

【００９０】

なお、この例は、ＵＩ画面の情報や連携サービスの包括指示書のひな形はフロー制御装置２０が保管し、随時指示入力装置１０に提供する構成であったが、それらＵＩ画面や包括指示書のひな形を指示入力装置１０に保管しておくこともできる。

【００９１】

フロー制御部２０４は、ユーザが要求した連携サービスを実現するために、連携サービスにおいて規定されるフローに従って各サーバ２５や指示入力装置１０に対して必要な処理の実行依頼を行う機能モジュールである。すなわち、連携サービスは、各サーバ２５が提供する１以上の処理（以下では単位ジョブとも呼ぶ）からなるフローとして定義され、フロー制御装置２０は、このフロー定義に示される単位ジョブを順に対応するサーバに依頼していく。ここで、各サーバの処

理結果は、必要に応じてフロー制御装置２０に返され、次の単位ジョブの処理対象データとしてフロー制御装置２０から対応するサーバへと送信される。フロー制御部２０４は、このような各サーバ、複合機への処理依頼と、これに対する処理結果の取得などの処理を実行する。

【００９２】

なお、指示入力装置１０が、連携サービスの指示受付機能の他にも処理機能を備え、この処理機能を連携サービスのために提供できる場合もある。この場合、指示入力装置１０は、その処理機能についてはアプリケーションサーバ２５の１つととらえることができる。

【００９３】

暗号・復号処理部２０６は、フロー制御装置２０からネットワーク３５に送信するデータに対して暗号化を行ったり、送信されてきた暗号化データを復号したりする機能モジュールであり、暗号・復号処理部１０８と同等の暗号化、復号化、電子署名及びその検証の機能を有する。

【００９４】

ここで暗号・復号処理部２０６は、指示入力装置１０や各サーバ２５などの装置や、各ユーザの公開鍵を保管しているか、又はネットワーク上の認証局等から取得する機能を備える。そして、データを送信する必要が生じた場合は、その送信先の装置やユーザの公開鍵を用いて暗号化を行う。

【００９５】

また、暗号・復号処理部２０６は、電子署名関連機能の一つとして、指示入力装置１０から送信されてきた包括指示書７０の全体に対するイニシエータ署名７６の検証を行う機能を備える。また、暗号・復号処理部２０６は、フロー制御装置２０の秘密鍵を備え、送信するデータに対してフロー制御装置２０の電子署名を付することができる。

【００９６】

通信制御部２１２は、フロー制御装置２０とネットワーク３５上の他の装置との通信のための各種制御処理を行う機能モジュールである。

【００９７】

以上、フロー制御装置２０の構成の一例を説明した。このようなフロー制御装置２０は、上述の各種の機能を記述したプログラムをコンピュータに実行させることによって実現できる。

【００９８】

次にアプリケーションサーバ２５について説明する。アプリケーションサーバ２５は、該サーバが提供するサービスのためのアプリケーションプログラム２５２と、ネットワーク３５上の他の装置との通信のための制御処理を実行する通信制御部２５４と、その通信の際の暗号化及び復号の処理を実行する暗号・復号処理部２５６とを備える。

【００９９】

サーバ２５の暗号・復号処理部２５６は、フロー制御装置２０又は他のサーバ２５から送られてきた包括指示書に対し、上述のイニシエータ署名検証を行う機能を備える。この署名検証が成功した場合、アプリケーション２５２による処理が実行される。

【０１００】

また暗号・復号処理部２５６は、該サーバ２５の処理によって得られたデータを暗号化する機能を備える。そのような処理結果のデータを、フロー制御装置２０又は他のサーバ２５に送る際には、その送り先の公開鍵を用いてそのデータを暗号化する。

【０１０１】

また、通信制御部２５４は、上述の第１の指示送信形態（図３）では、アプリケーション２５２の処理結果をフロー制御装置２０に送信する処理を行う。また通信制御部２５４は、第２の指示送信形態（図３）では、次のサーバ２５に対する包括指示書６０（及び、必要に応じ、処理結果のデータ）を送信するための上述の処理を実行する。

【０１０２】

以上説明した指示入力装置１０及びサーバ２５、及びフロー制御装置介在型のシステム構成の場合は更にフロー制御装置２０により、上述の連携サービスのフローが実現されると共に、そのフローにおける各サーバ２５への指示書の秘密を

守る処理が行われる。

【図面の簡単な説明】

【図１】　連携サービスを提供するシステムの構成の一例を示す図である。

【図２】　連携サービスを提供するシステムの構成の別の例を示す図である

【図３】　連携サービスにおける各サーバへの指示書の第１の送信形態を説明するための図である。

【図４】　連携サービスにおける各サーバへの指示書の第２の送信形態を説明するための図である。

【図５】　本実施形態によるイニシエータ署名を施した包括指示書のデータ構造の一例を模式的に示す図である。

【図６】　平文の包括指示書の例を示す図である。

【図７】　本実施形態によるイニシエータ署名を施した包括指示書の例を示す図である。

【図８】　指示入力装置が作成する包括指示書のデータ構造の別の例を模式的に示す図である。

【図９】　本実施形態によるイニシエータ署名を施した包括指示書の別の例を示す図である。

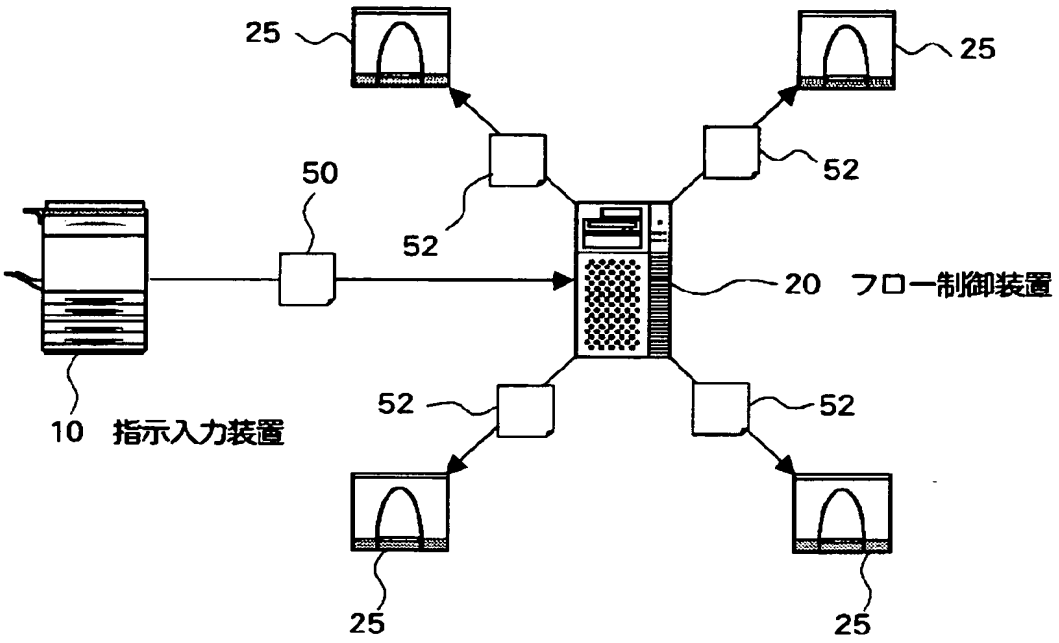
【図１０】　連携サービスを提供するシステムを構成する各装置の内部構造の例を示す図である。

【符号の説明】

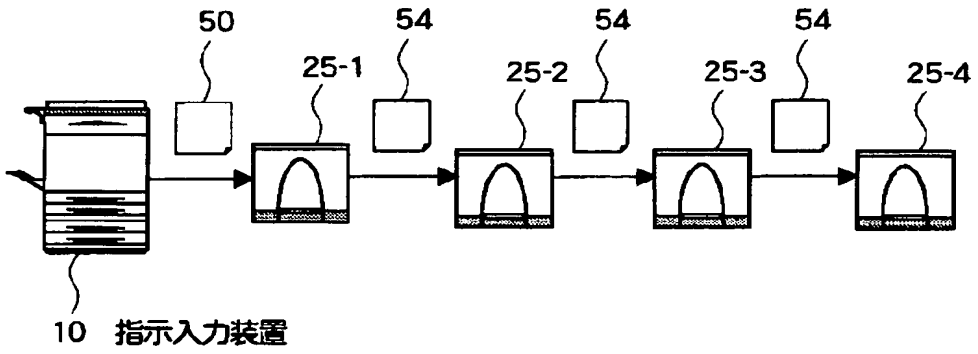
１０　指示入力装置、２０　フロー制御装置、２５　アプリケーションサーバ、５２，５４　指示書、６０，７０　包括指示書、６２　個別指示書、７２－１，７２－２，７２－３　署名済み個別指示書、７４－１，７４－２，７４－３，７６　イニシエータ署名。

【書類名】　　図面

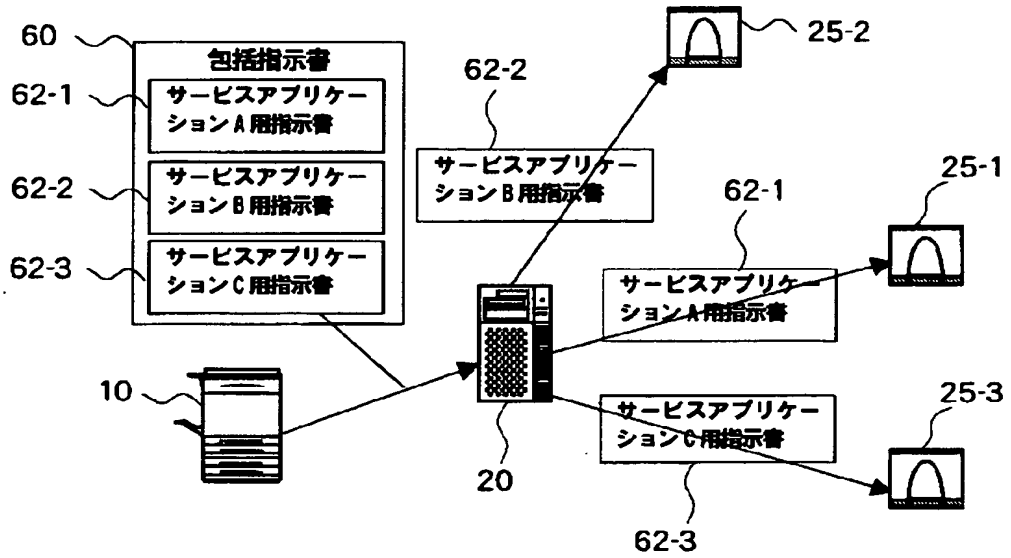
【図１】


25
25
50
52
52
20　フロー制御装置
52
52
10　指示入力装置
25
25

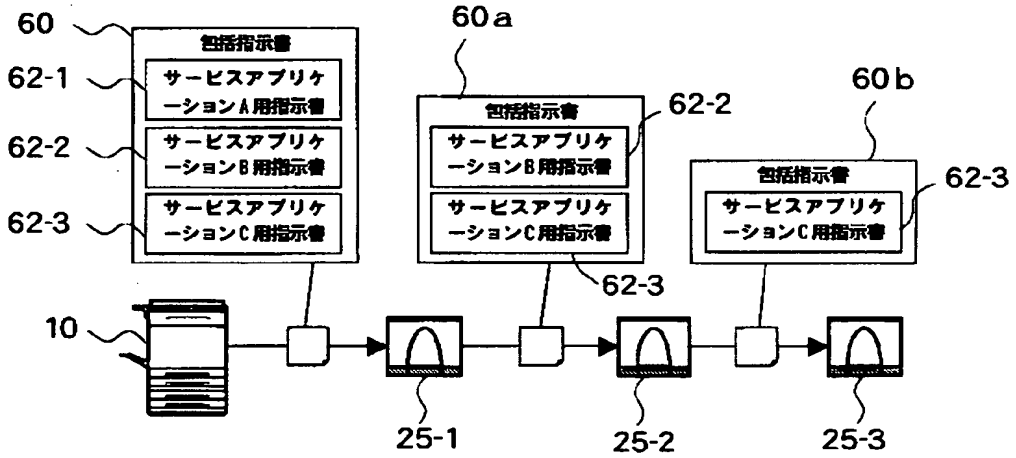
【図２】


50
54
54
54
25-1
25-2
25-3
25-4
10　指示入力装置

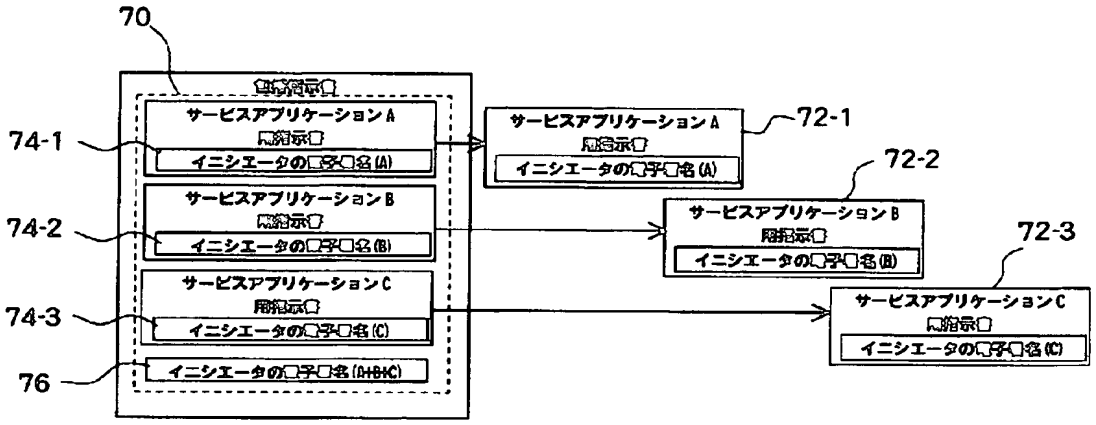
【図３】


60
包括指示書
62-1
サービスアプリケーションA用指示書
62-2
サービスアプリケーションB用指示書
62-3
サービスアプリケーションC用指示書
10
20
62-2
サービスアプリケーションB用指示書
25-2
62-1
サービスアプリケーションA用指示書
25-1
サービスアプリケーションC用指示書
25-3
62-3

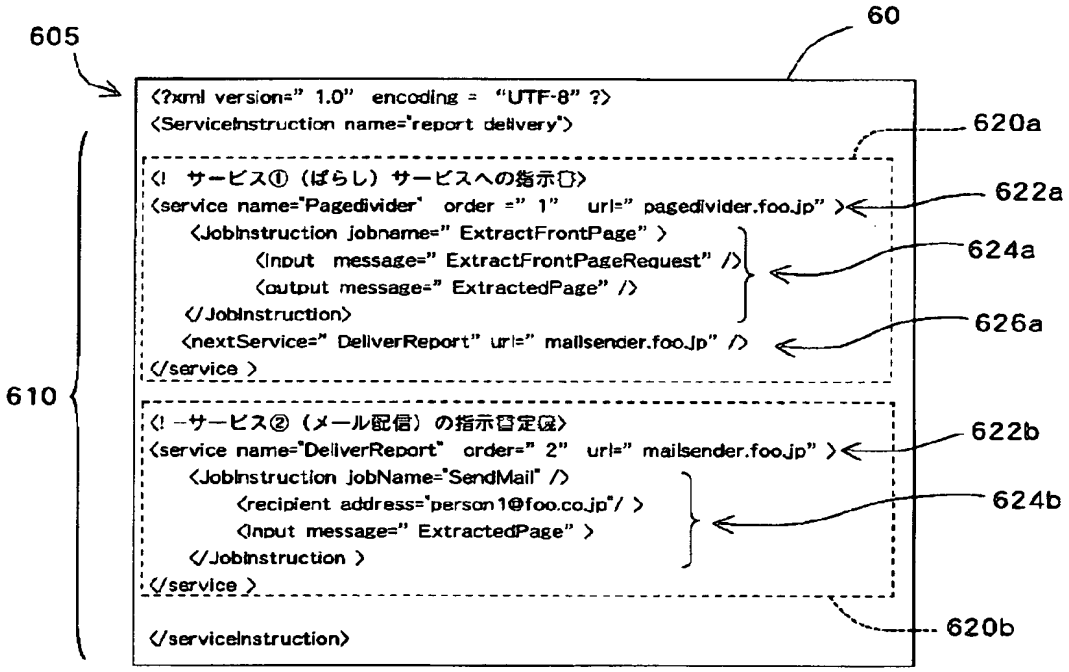
【図４】


60
包括指示書
62-1
サービスアプリケーションA用指示書
62-2
サービスアプリケーションB用指示書
62-3
サービスアプリケーションC用指示書
10
60a
包括指示書
62-2
サービスアプリケーションB用指示書
サービスアプリケーションC用指示書
62-3
60b
包括指示書
62-3
サービスアプリケーションC用指示書
25-1
25-2
25-3

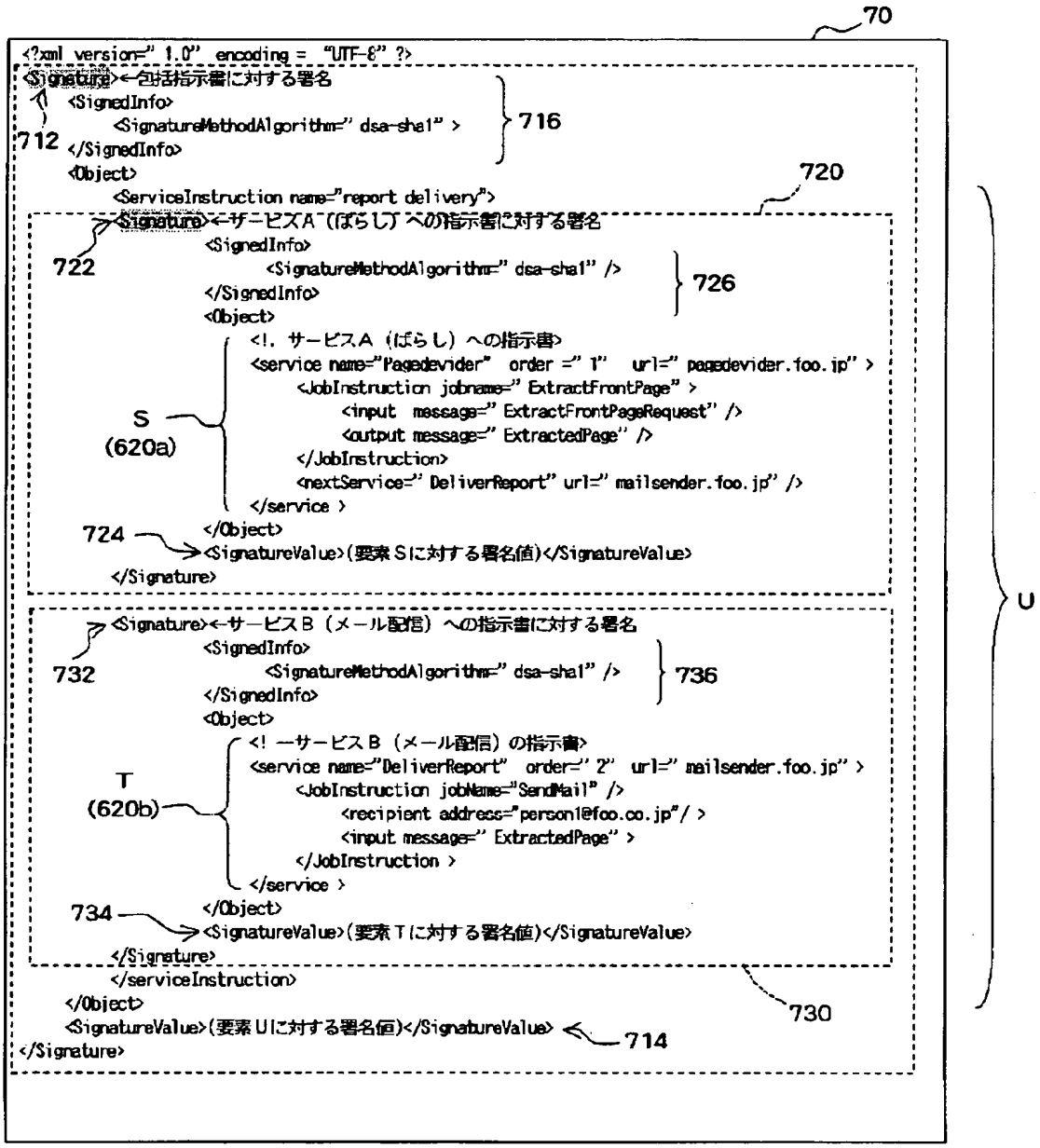
【図５】


70
サービスアプリケーションA
起動指示
イニシエータの□字□名(A)
サービスアプリケーションB
起動指示
イニシエータの□字□名(B)
サービスアプリケーションC
起動指示
イニシエータの□字□名(C)
イニシエータの□字□名(A+B+C)
74-1
74-2
74-3
76
72-1
72-2
72-3

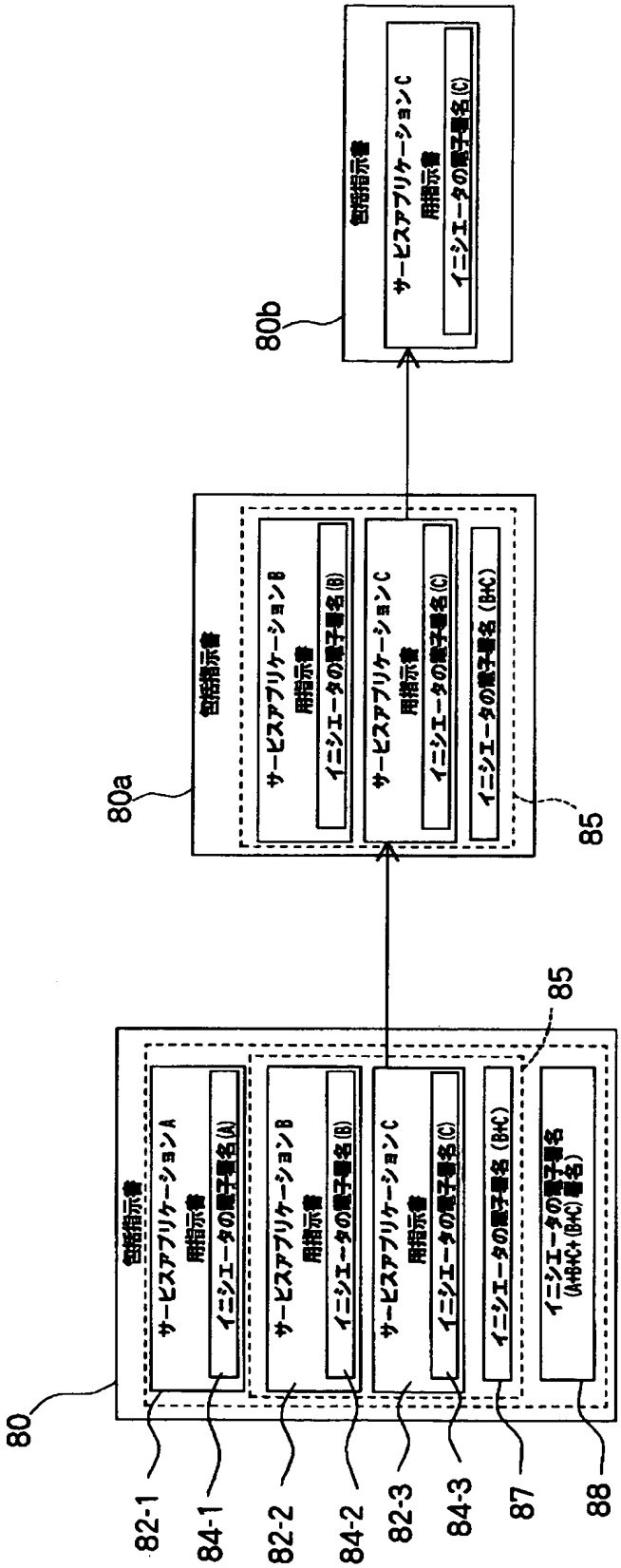
【図６】


605
60
<?xml version=" 1.0" encoding = "UTF-8" ?>
<ServiceInstruction name="report delivery">
620a
<! サービス① (ばらし) サービスへの指示□>
<service name="Pagedivider" order =" 1" url=" pagedivider.foo.jp" >
622a
<JobInstruction jobname=" ExtractFrontPage" >
<Input message=" ExtractFrontPageRequest" />
<output message=" ExtractedPage" />
624a
</JobInstruction>
<nextService=" DeliverReport" url=" mailsender.foo.jp" />
626a
</service >
610
<! -サービス② (メール配信) の指示設定例>
<service name="DeliverReport" order=" 2" url=" mailsender.foo.jp" >
622b
<JobInstruction jobName="SendMail" />
<recipient address="person1@foo.co.jp"/ >
<Input message=" ExtractedPage" >
624b
</JobInstruction >
</service >
620b
</ServiceInstruction>

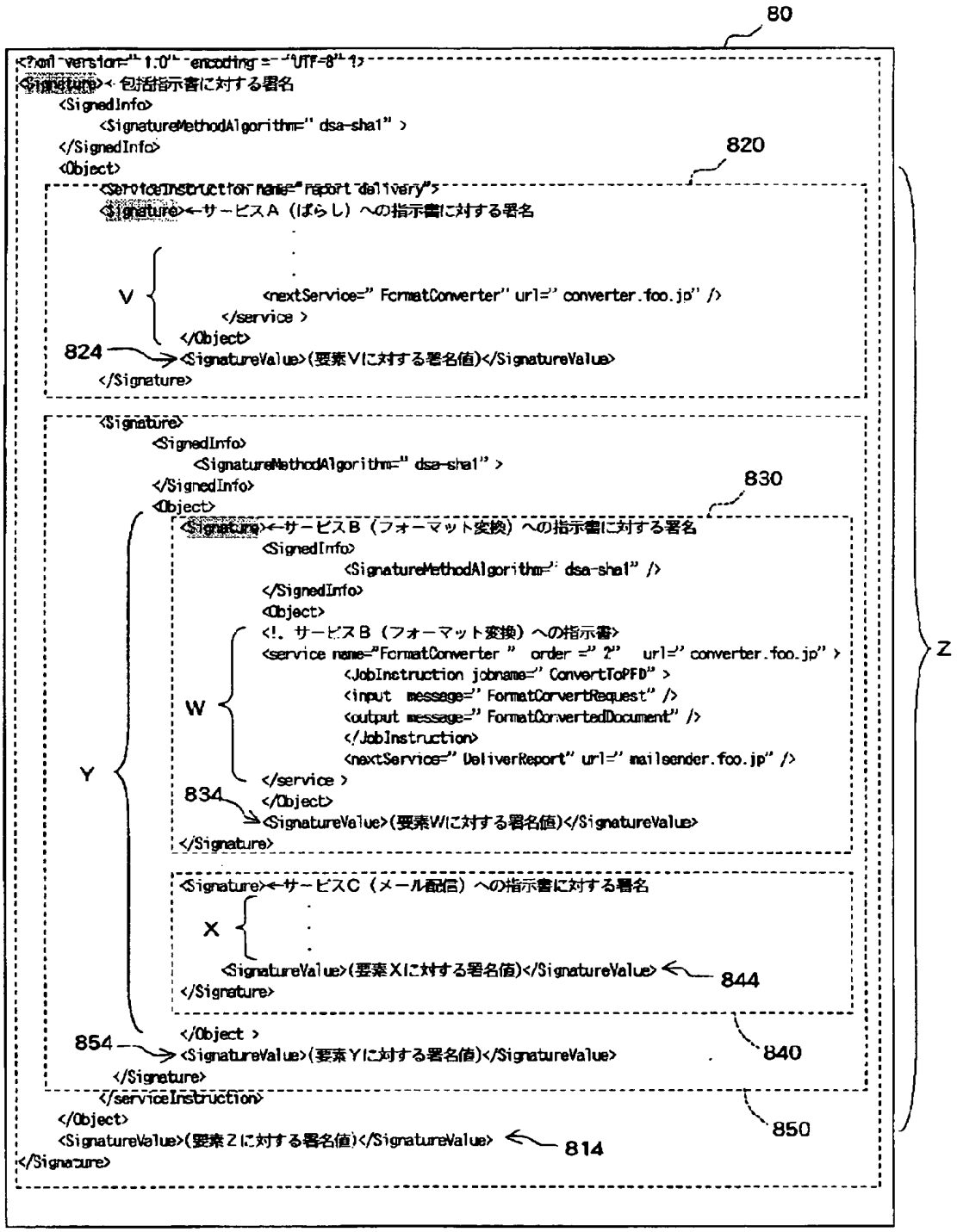
【図７】


70
<?xml version=" 1.0" encoding = "UTF-8" ?>
<Signature>←包括指示書に対する署名
<SignedInfo>
<SignatureMethodAlgorithm=" dsa-sha1" >
716
712
</SignedInfo>
<Object>
720
<ServiceInstruction name="report delivery">
<Signature>←サービスA（ばらし）への指示書に対する署名
722
<SignedInfo>
<SignatureMethodAlgorithm=" dsa-sha1" />
726
</SignedInfo>
<Object>
<!. サービスA （ばらし）への指示書>
<service name="Pagedevider" order =" 1" url=" pagedevider.foo.jp" >
S
(620a)
<JobInstruction jobname=" ExtractFrontPage" >
<input message=" ExtractFrontPageRequest" />
<output message=" ExtractedPage" />
</JobInstruction>
<nextService=" DeliverReport" url=" mailsender.foo.jp' />
</service >
724
</Object>
<SignatureValue>(要素Sに対する署名値)</SignatureValue>
</Signature>
<Signature>←サービスB （メール配信） への指示書に対する署名
732
<SignedInfo>
<SignatureMethodAlgorithm=" dsa-sha1" />
736
</SignedInfo>
<Object>
<! ーサービスB （メール配信）の指示書>
<service name="DeliverReport" order=" 2" url=" mailsender.foo.jp" >
T
(620b)
<JobInstruction jobName="SendMail" />
<recipient address="person1@foo.co.jp"/ >
<input message=" ExtractedPage" >
</JobInstruction >
</service >
734
</Object>
<SignatureValue>(要素Tに対する署名値)</SignatureValue>
</Signature>
730
</serviceInstruction>
</Object>
<SignatureValue>(要素Uに対する署名値)</SignatureValue>
714
</Signature>
U

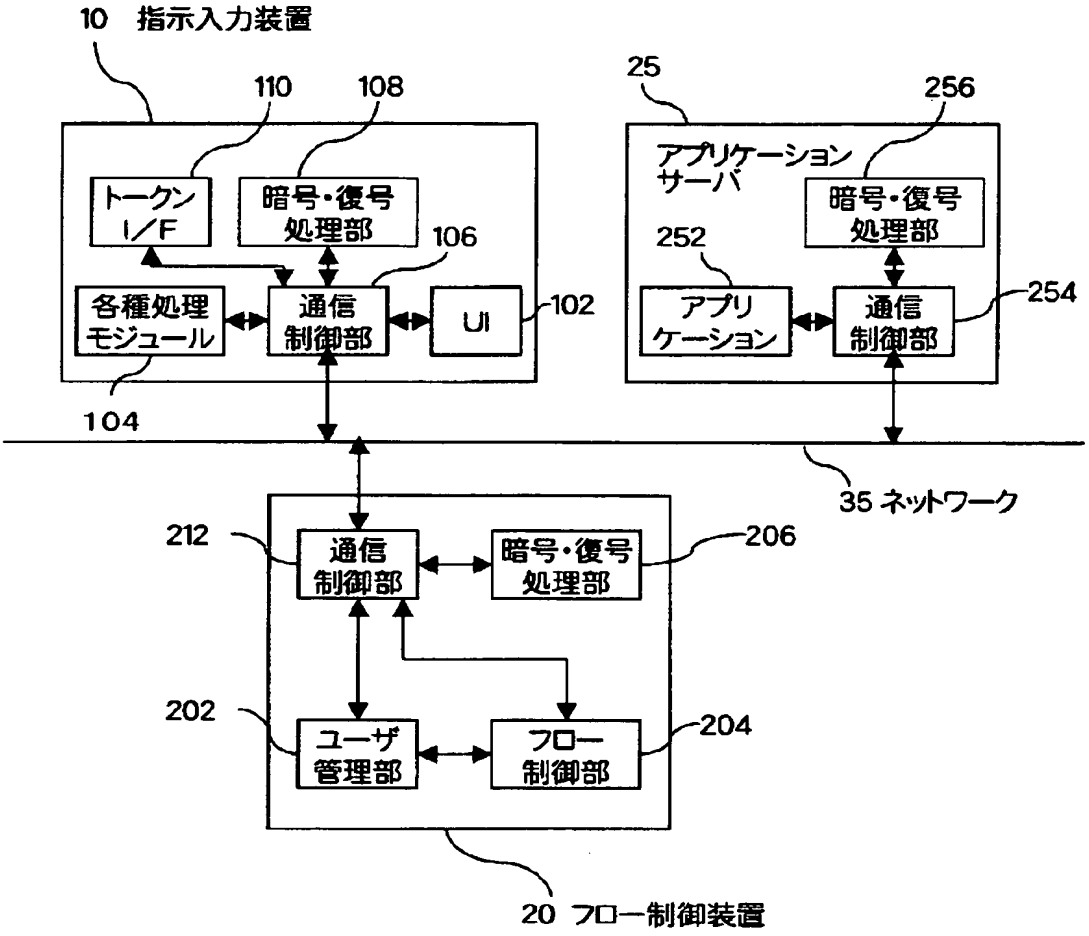
【図８】


包括指示書
サービスアプリケーションC
用指示書
イニシエータの電子署名(C)
80b
包括指示書
サービスアプリケーションB
用指示書
イニシエータの電子署名(B)
サービスアプリケーションC
用指示書
イニシエータの電子署名(C)
イニシエータの電子署名(B+C)
80a
85
包括指示書
サービスアプリケーションA
用指示書
イニシエータの電子署名(A)
サービスアプリケーションB
用指示書
イニシエータの電子署名(B)
サービスアプリケーションC
用指示書
イニシエータの電子署名(C)
イニシエータの電子署名(B+C)
イニシエータの電子署名
(A+B+C+(B+C)署名)
85
80
82-1
84-1
82-2
84-2
82-3
84-3
87
88

【図９】


<?xml version="1.0" encoding="UTF-8"?>
<Signature>←包括指示書に対する署名
<SignedInfo>
<SignatureMethodAlgorithm=" dsa-sha1" >
</SignedInfo>
<Object>
<ServiceInstruction name="report delivery">
<Signature>←サービスＡ（ばらし）への指示書に対する署名
V
<nextService=" FormatConverter" url=" converter.foo.jp" />
</service >
</Object>
824
<SignatureValue>(要素Vに対する署名値)</SignatureValue>
</Signature>
<Signature>
<SignedInfo>
<SignatureMethodAlgorithm=" dsa-sha1" >
</SignedInfo>
<Object>
<Signature>←サービスＢ（フォーマット変換）への指示書に対する署名
<SignedInfo>
<SignatureMethodAlgorithm=" dsa-sha1" />
</SignedInfo>
<Object>
<!. サービスＢ（フォーマット変換）への指示書>
<service name="FormatConverter " order =" 2" url=" converter.foo.jp" >
<JobInstruction jobname=" ConvertToPFD" >
W
<input message=" FormatConvertRequest" />
<output message=" FormatConvertedDocument" />
</JobInstruction>
<nextService=" DeliverReport" url=" mailsender.foo.jp" />
Y
</service >
834
</Object>
<SignatureValue>(要素Wに対する署名値)</SignatureValue>
</Signature>
<Signature>←サービスＣ（メール配信）への指示書に対する署名
X
<SignatureValue>(要素Xに対する署名値)</SignatureValue>
844
</Signature>
</Object >
854
<SignatureValue>(要素Yに対する署名値)</SignatureValue>
840
</Signature>
</ServiceInstruction>
850
</Object>
<SignatureValue>(要素Ｚに対する署名値)</SignatureValue>
814
</Signature>
80
820
830
Z

【図１０】


10　指示入力装置
110
108
トークン I/F
暗号・復号処理部
106
各種処理モジュール
通信制御部
UI
102
104
25
256
アプリケーションサーバ
暗号・復号処理部
252
アプリケーション
通信制御部
254
35 ネットワーク
212
通信制御部
暗号・復号処理部
206
202
ユーザ管理部
フロー制御部
204
20 フロー制御装置

【書類名】　　要約書

【要約】

【課題】　各サーバへの指示を示した指示書をそれらサーバ間で受け渡しながら各サーバが指示書内の各自の指示を実行することで、連携サービスを提供するシステムにおいて、各サーバがサービス指示者の署名を検証できるようにする。

【解決手段】　サービス指示者から指示を受け付けた指示入力装置は、各サーバの処理内容を示した指示書に対して指示者又は当該装置の電子署名（イニシエータ署名７４）を付して署名済み個別指示書７２を作成する。そしてサービスに利用するすべてのサーバの署名済み個別指示書７２を併合したものに対してイニシエータ署名７６を付して包括指示書７０を作成する。包括指示書７０は、それらサーバを制御するフロー制御装置に送られる。フロー制御装置はイニシエータ署名７６によりその包括指示書７０の真正性等を検証する。検証が成功すると、フロー制御装置は各サーバに対応する署名済み個別指示書７２を送信する。

【選択図】　　図５

特願２００３－０８２３２３

出　願　人　履　歴　情　報

識別番号　　［０００００５４９６］

１．変更年月日　　１９９６年　５月２９日
［変更理由］　　住所変更
住　所　　東京都港区赤坂二丁目１７番２２号
氏　名　　富士ゼロックス株式会社